AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

Claim 1 (Original): A method comprising:

detecting presence of an event;

receiving an inbound packet from a network; and

selectively processing the packet using a software process or an interrupt-driven service routine based on the detection of the event.

Claim 2 (Original): The method of claim 1, wherein the event comprises a network attack.

Claim 3 (Currently Amended): The method of claim 1, wherein selectively processing the packet comprises:

invoking the service routine using a software interrupt when the event is not detected; and

invoking the software process using a wakeup signal upon the detection of the event.

Claim 4 (Original): The method of claim 1, wherein detecting the presence of an event comprises detecting the event based on a traffic level of inbound packets received by a router.

Claim 5 (Currently Amended): A method for processing a network packet comprising:

receiving inbound packets from a network;

~~processing the packets using a software process; and~~

setting a rate-limiting operating mode based on a traffic level of the inbound packets; and

selectively invoking a packet service routine based on the rate-limiting operating mode by:

calling the packet service routine from a software process without issuing an interrupt when the traffic level of the inbound packets exceeds a threshold and controlling a usage rate by which the software process uses computing resources to process the packets, and

issuing a software interrupt to invoke the packet service routine as an interrupt-driven service routine when the traffic level of the inbound packets does not exceed the threshold.

~~controlling a usage rate by which the software process uses computing resources to process the packets.~~

Claim 6 (Original): The method of claim 5, wherein controlling the usage rate comprises determining an execution period that the software process has executed without a context switch.

Claim 7 (Original): The method of claim 6, wherein controlling the usage rate comprises pausing execution of the software process for a sleep period when the execution period exceeds a threshold.

Claim 8 (Currently Amended): The method of claim 7, wherein pausing execution of the software process comprises dynamically adjusting the sleep period during a ~~the~~ network attack.

Claim 9 (Original): The method of claim 5, wherein processing the packets comprises invoking a packet service routine from the software process.

Claim 10 (Canceled)

Claim 11 (Currently Amended): The method of claim ~~10~~5, wherein invoking the packet service routine comprises selecting a pointer to the ~~PSR~~packet service routine from a table of pointers to invoke packet service routines supporting a number of network protocols in response to an interrupt.

Claim 12 (Original): The method of claim 5, further comprising detecting a presence of a network attack.

Claim 13 (Original): The method of claim 12, wherein detecting the presence of the network attack comprises detecting the network attack based on a traffic level of inbound packets.

Claim 14 (Original): The method of claim 12, wherein detecting the presence of a network attack comprises detecting a denial of service (DOS) attack.

Claim 15 (Original): A method of processing network packets within a routing device comprising:

selecting between a first mode of processing inbound packets using interrupt service routines and a second mode of processing the inbound packets using a software process executing within an operating environment provided by a multi-tasking operating system; and

processing a set of packets within a network routing device according to the selected mode.

Claim 16 (Original): The method of claim 15, further comprising detecting a presence of a network attack, wherein selecting between the first and second modes comprises selecting between the first and second modes based on the detection of the network attack.

Claim 17 (Original): The method of claim 16, wherein detecting the presence of the network attack comprises detecting the network attack based on a traffic level of inbound packets.

Claim 18 (Original): The method of claim 16, wherein detecting the presence of a network attack comprises detecting a denial of service (DOS) attack.

Claim 19 (Currently Amended): A computer-readable medium comprising instructions for causing a programmable processor to:

receive inbound packets from a network;

~~process the packets using a software process executing on the programmable processor; and~~

set a rate-limiting operating mode based on a traffic level of the inbound packets;

selectively invoke a packet service routine based on the rate-limiting operating mode by:

calling the packet service routine from a software process without issuing an interrupt when the traffic level of the inbound packets exceeds a threshold and controlling a usage rate by which the software process uses computing resources to process packets, and

issuing a software interrupt to invoke the packet service routine as an interrupt-driven service routine when the traffic level of the inbound packets does not exceed the threshold.

~~control a usage rate by which the software process uses computing resources to process packets.~~

Claim 20 (Canceled).

Claim 21 (Canceled).

Claim 22 (Currently Amended): The computer-readable medium of claim 19, wherein the instructions cause the processor to select a pointer to the packet service routine from a table of pointers to invoke packet service routines supporting a number of network protocols in response to an interrupt.

Claim 23 (Original): The computer-readable medium of claim 19, wherein the instructions cause the processor to detect a presence of a network attack.

Claim 24 (Original): The computer-readable medium of claim 23, wherein the instructions cause the processor to detect the network attack based on a traffic level of inbound packets.

Claim 25 (Original): The computer-readable medium of claim 23, wherein the instructions cause the processor to detect a denial of service (DOS) attack.

Claim 26 (Original): A routing device comprising:

a detection module to detect a presence of a network attack;

a network interface to receive a packet from the network; and

a routing engine to selectively process the packet using a software process or an interrupt-driven service routine based on the detection of the network attack.

Claim 27 (Original): The routing device of claim 26, where the detection module includes a counter indicating a number of packets processed for a network protocol, wherein the detection module enables a rate-limiting operating mode of the routing engine when the counter exceeds a protocol-specific threshold.

Claim 28 (Original): The routing device of claim 26, wherein the detection module comprises a network service routine invoked in response to a hardware interrupt from the network interface.

Claim 29 (Original): The routing device of claim 26, further comprising:

a set of packet service routines to service inbound packets in accordance with a plurality of network protocols; and

an operating system to invoke one of the packet service routines to invoke the software process in response to wakeup signal when the network attack is detected, and to invoke the software process in response to a software interrupt when the network attack is not detected.

Claim 30 (Original): The routing device of claim 26, wherein the software process controls a usage rate of computing resources to process the packets.

Claim 31 (Currently Amended): The routing device of claim 30, wherein the software process controls usage rate of computing resources by determining an execution period that the software process ~~processes~~ has executed without a context switch, and pausing execution of the software process for a sleep period when the execution period exceeds a threshold.

Claim 32 (Original): The routing device of claim 31, wherein the software process dynamically adjusts the sleep period during the network attack.

Claim 33 (Original): The routing device of claim 26, wherein the detection module detects the presence of the network attack based on a traffic level of inbound packets.

Claim 34 (Original): The routing device of claim 26, wherein detection module detects the presence of a denial of service (DOS) attack.

Claim 35 (Currently Amended): The routing device of claim ~~36~~29, further comprising a table of pointers to invoke the packet service routines in response to an interrupt.